UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/713,980	11/14/2003	Brian D. Swander	14917.0474US01	3167

27488 7590 04/21/2008

MERCHANT & GOULD (MICROSOFT)
P.O. BOX 2903
MINNEAPOLIS, MN 55402-0903

EXAMINER	
PALIWAL, YOGESH	
ART UNIT	PAPER NUMBER
2135	
MAIL DATE	DELIVERY MODE
04/21/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/713,980	SWANDER ET AL.	
	Examiner	Art Unit	
	YOGESH PALIWAL	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 January 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-9,18-22,26 and 27* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-9,18-22,26 and 27* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *12/7/2007*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

- Applicant's amendment filed on 01/10/2008 has been entered. Applicant has amended claims 1, 3, 7, 18, 19, 20, 21, and 22 and added claims 26 and 27. Currently claims 1-9, 18-22 and 26-27 are pending in this application.

Docketing

1. Please note that the application has been re-docketed to different examiner. Please refer all future communications regarding this application to the examiner of record using the information supplied in the final section of the office action.

Response to Arguments

2. Applicant's arguments filed 1/10/2008 have been fully considered but they are not persuasive for following reasons:

- Applicant argues: "Faucher fails suggest conducting a main mode negotiation for establishing the secure path and selecting the set of security parameters including a security protocol; and conducting a quick mode negotiation for deriving a set of keys usable with the security protocol, as recited in claim 1. During the December 13, 2007 interview, the Examiner maintained that the calculation of the first session key in Faucher constituted a "main mode" and the calculation of the second session key in Faucher constituted a "quick mode." Applicants disagree; however, even if Faucher did teach conducting a main mode negotiation and conducting a quick mode negotiation, the reference still fails to teach or suggest all of the limitations of independent claim 1."

- Regarding Claims 1 and 18, examiner is interpreting calculation of the first session key in Faucher constituting a "main mode" and the calculation of the final key that include the Diffie-Hellman key exchange in Faucher constituting a "quick mode" negotiation see (see Faucher, Column 10 lines 1-13).

- Applicant further argues: "For example, Faucher also fails to teach or suggest: wherein at least one message that comprises at least part of the quick mode negotiation is sent during the main mode negotiation and a quick mode pseudo random number is exchanged between the responder and the initiator. (emphasis added). As discussed above, Faucher teaches generating a first session key using information contained in certificates passed between the computing devices. (See Faucher, col. 9, 1.66 - col. 10, 1. 13). Second, Faucher discloses generating a second session key with a "straight Diffie-Hellman key exchange." (Faucher, col. 10, 11. 13-15). However, **at no point does the reference teach or suggest that a least one message that comprises at least part of the Diffie-Hellman key exchange used to create the second session key is sent during the certificate exchange used to create the first session key**. In fact, Faucher teaches just the opposite: "[The first session key is calculated], thus validating the remote terminal. The procedure continues with a straight Diffie-Hellman key exchange to generate a second session key." (See Faucher, col. 10, 11.2-15, emphasis added). Thus, the reference fails to teach or suggest, at least, wherein at least one message that comprises at least part of the quick mode negotiation is sent during the main mode negotiation and a quick mode pseudo random number is exchanged between the responder and the initiator."

- Examiner would like to point to Column 10, lines 13-16 of Faucher reference which recites, "The procedure continues with a straight Diffie-Hellman key exchange to generate a second session key.

These two session key are combined to form the final session key". Applicant should note that the first session key exchanged during main mode is actually needed to derive the final session key. Examiner is interpreting the Diffie-Hellman key exchange and the generation of the final key as a quick mode, it can be seen that the generation of final key requires a first session key exchanged during the main mode negotiation. Therefore, Faucher still discloses the limitation of "wherein at least one message that comprises at least part of the quick mode negotiation is sent during the main mode negotiation and a quick mode pseudo random number is exchanged between the responder and the initiator".

Claim Rejections - 35 USC § 103

3. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

Claims 1-9 and 18-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Faucher (5,515,441), hereinafter "Faucher", in view of Inoue et al (6,170,057 B1), hereinafter "Inoue".

In reference to ***claims 1 and 18***, Faucher discloses a communication system in which a node may communicate over insecure channels with any of a plurality of terminals (abstract). Faucher teaches conducting a main mode, certificate exchange, negotiation for establishing the secure path (column 10 lines 1-13); conducting a quick mode, Diffie-Hellman key exchange including the calculation of final session key, negotiation for deriving a set of keys usable with the security protocol (column 10 line 13 to column 11 line 2). Wherein at least one message that comprises at least part of the quick mode negotiation is sent

during the main mode negotiation (See Colum 10, lines 15-16, "These two session keys are combined to form the final session key", for detailed explanation please refer to the “response to argument section”) and a quick mode pseudo random number is exchanged between the responder and the initiator (column 10 line 13 to column 11 line 2).

However Faucher does not expressly disclose selecting the set of security parameters including a security protocol and establishing inbound and outbound protocol security association.

Inoue teaches a mobile computer and a packet encryption and authentication method which are capable of controlling an activation of a packet encryption and authentication device belonging to the mobile computer according to the security policy at the visited network (abstract). Inoue teaches negotiation for establishing the secure path and selecting the set of security parameters including a security protocol (column 7 lines 1-11). And wherein a protocol security process establishes inbound and outbound protocol security associations (column 7 lines 20-29.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher. One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

In reference to ***claim 2 and 19*** Faucher teaches further comprising conducting a first user mode for authenticating a first user associated with the initiator or responder (column 10 lines 1-10).

In reference to ***claims 3 and 20*** Faucher teaches a system wherein the initiator and the responder exchange authentication data that is calculated by application of a hash function incorporating a secret key on data exchanged during the main mode negotiation (column 10 lines 3-8).

In reference to ***claim 4*** the system of Faucher comprising conducting a second user mode for authenticating a second user associated with the initiator or the responder (column 10 lines 1-10).

In reference to ***claim 5*** Faucher does not discloses a system wherein a set of proposed security parameters are used for selection of the parameters used for communication.

The system of Inoue discloses a system wherein the main mode comprises sending the initiator to the responder, a set of proposed security parameters and authentication data; selecting, by the responder, the set of security parameters from the set of proposed security parameters; and sending the set of security parameters from the responder to the initiator (column 7 lines 20-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher. One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

In reference to ***claims 6 and 21*** Faucher teaches a system wherein the initiator identifies a public key of the responder prior to the main mode negotiation and wherein at least a portion a first message sent from the initiator to the responder is encrypted using the public key (Fig 6).

In reference to ***claim 8*** Faucher teaches further comprising exchanging Diffie Hellman key data between the initiator and the responder during main mode for deriving keys for use with an encryption algorithm (column 10 lines 1-20).

In reference to ***claim 9*** Faucher does not disclose exchanging a pair of notify payloads between the initiator and the responder wherein the pair of notify payloads are used by the protocol security process for establishing the protocol security associations.

further comprising exchanging a pair of notify payloads between the initiator and the responder; wherein the pair of notify payloads are used by the protocol security process for establishing the protocol security associations (Fig. 4).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher. One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

In reference to ***claims 7 and 22*** Faucher does not disclose the mode wherein a group advertisement from the initiator to the responder; and comparing the group advertisement to a set of authorized groups; and sending a response from the responder to the initiator. The group advertisement corresponds to the security parameters of the remote network gateway.

Inoue discloses a system wherein the main mode comprises sending a group advertisement from the initiator to the responder; and comparing the group advertisement to a set of authorized groups; and sending a response from the responder to the initiator (column 7 lines 20-65).

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher. One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

In reference to ***claim 26***, Faucher discloses a method for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method comprising:

sending, from the initiator (see Fig. 5, Terminal A transmitting certificate to Terminal B), a first message, wherein the first message comprises part of a main mode negotiation and the main mode negotiation comprises establishing the secure path (see Fig. 5, exchange of certificates and also at Column 8, lines 10-19) and the main mode negotiation comprises establishing the secure path (see Column 8, lines 10-19);

receiving, at the initiator (See Fig. 5, Terminal A receiving public random component X^{Rb} mod p of terminal B encrypted with the public key of terminal A (PK_a)) , a second message, wherein the second message comprises at least part of a quick mode negotiation (See Fig. 5, Terminal A receiving public random component XR_b mod p of terminal B encrypted with the public key of terminal A (PK_a)) and the

quick mode negotiation comprises deriving a set of keys usable with the security protocol (see Fig. 5, "session key");

sending, from the initiator, a third message after receiving the second message, wherein the third message comprises at least part of the main mode negotiation (See Fig. 5, Terminal A transmit public random component X^{Ra} mod p encrypted with the public key of terminal B (PK_b) that it received from the certificate of terminal B during the main mode negotiation);

However Faucher does not expressly disclose selecting the set of security parameters including a security protocol and establishing inbound and outbound protocol security association.

Inoue teaches a mobile computer and a packet encryption and authentication method which are capable of controlling an activation of a packet encryption and authentication device belonging to the mobile computer according to the security policy at the visited network (abstract). Inoue teaches negotiation for establishing the secure path and selecting the set of security parameters including a security protocol (column 7 lines 1-11). And wherein a protocol security process establishes inbound and outbound protocol security associations (column 7 lines 20-29.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher. One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

In reference to ***claim 27***, Faucher discloses a method for negotiating a set of security parameters usable by an initiator and a responder to create a secure path over a network for exchanging information, the method comprising:

receiving, at the responder (Terminal B), a first message (See Fig. 5, Terminal B receive TC_a) , wherein the first message comprises at least part of a main mode negotiation (see Fig. 5, exchange of certificates and also at Column 8, lines 10-19) and the main mode negotiation comprises establishing the secure path (see Column 8, lines 10-19);

sending, from the responder, a second message, wherein the second message comprises at least part of the main mode negotiation and at least part of a quick mode negotiation (see Fig. 5, terminal B sends public random component X^{Rb} mod p encrypted with the public key of terminal A (PK_a) that it received from the certificate during the main mode negotiation) and wherein the quick mode negotiation comprises deriving a set of keys usable with the security protocol (see Fig. 5, "session key"); and

However Faucher does not expressly disclose selecting the set of security parameters including a security protocol and establishing inbound and outbound protocol security association.

Inoue teaches a mobile computer and a packet encryption and authentication method which are capable of controlling an activation of a packet encryption and authentication device belonging to the mobile computer according to the security policy at the visited network (abstract). Inoue teaches negotiation for establishing the secure path and selecting the set of security parameters including a security protocol (column 7 lines 1-11). And wherein a protocol security process establishes inbound and outbound protocol security associations (column 7 lines 20-29.

At the time the invention was made, it would have been obvious to a person of ordinary skill in the art to add the method of selecting security parameters as disclosed by Inoue in the system of Faucher.

One of ordinary skill in the art would have been motivated to do this because due to technological developments in mobile computing a user carries along a portable computer terminal and makes communication while moving over networks and therefore networks are less centralized and more distributed. Thus it would be advantageous to be able to have a scheme to negotiate security parameters (column 1 lines 29-51).

Conclusion

4. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YOGESH PALIWAL whose telephone number is (571)270-1807. The examiner can normally be reached on M-F: 7:30 AM - 5:00 PM EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. P./
Examiner, Art Unit 2135
/KIMYEN VU/
Supervisory Patent Examiner, Art Unit 2135